IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Edward W. Kohler, Jr., et al.	Art Unit	: 2155
Serial No.	: 09/931,487	Examiner	: Shawki Saif Ismail
Filed	: August 16, 2001	Conf. No.	: 3664
Title	: THWARTING SOURCE ADDRESS SPOOFING-BASED DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. §41.41, Applicant responds to the Examiner's Answer as follows:

Argument A (Claim 1)

The examiner argues that:

> **Yavatkar teaches analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process.**[1]

The claim which argument A addresses is claim 1. Claim 1 includes the features of: "... sending queries to data collectors, deployed at different points in a network ... the queries to request the statistical information from at least some of the data collectors... and processing the statistical information to determine the source of suspicious network traffic sent to the data center." Neither Yavatkar nor the examiner's assessment of Yavatkar, as quoted above, describes or suggests these features.

The examiner recognizes this and resorts to an unsupportable interpretation of Yavatkar. The examiner argues: "... **Examiner is equating the launching of the various types of bloodhound agents to**

[1] Examiner's Answer page 10

launching various types of queries to each bloodhound agent upon its creation based on the type of attack detected." [2]

The examiner reminds Appellant that: **"The appellant is reminded that the claims must be given their broadest reasonable interpretation."**[3]

Appellant contends that the examiner's construction of Yavatkar is "unreasonable." According to *Morris*, the examiner must apply the broadest "reasonable" meaning to terms "in their ordinary usage as they would be understood by one of ordinary skill in the art."[4] The person of ordinary skill, indeed the person skilled in this art would not equate the launch of "bloodhound agents", which is mere jargon for the remote instantiation of objects in a object oriented computing environment, as taught by Yavatkar to "sending queries to data collectors ... that ... collect statistical information on network packets sent over the network ... to request the statistical information from at least some of the data collectors."

This conclusion is compelled since, Yavatkar describes the function of watchdog agent, which does not involving querying the bloodhound agents nor collecting statistical information from the bloodhound agents,[5] but rather to trace paths of attacks.

While, Yavatkar envisions distributed monitoring by watchdog agents[6] that instantiate bloodhound agents[7] to follow paths of attacks[8] Appellant, in contrast, envisions an arrangement to process statistical information derived from network packet flows seen by distributed data collectors (e.g., deployed at different points in a network). Given the ordinary meanings that one skilled in the art would apply to the terms "queries" and "launching of objects," and indeed, the

---

[2] Id. page 11.
[3] Id.
[4] Appellant contends that the Examiner improperly ignores Appellant's specification to guide the examiner to give the claims their broadest reasonable construction. The Federal Circuit in *In re Morris* 127 F.3d 1048 (Fed. Cir. 1997). requires the examiner to apply the Court's guidance on what "reasonable" means:

> "Since it would be unreasonable for the PTO to ignore any interpretive guidance afforded by the applicant's written description, either phrasing connotes the same notion: as an initial matter, the PTO applies to the verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, *taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description* contained in the applicant's specification." [emphasis supplied]

[5] Yavatkar col. 16, line 46-49. "The watchdog agent waits for each bloodhound agent to report, destroys each bloodhound agent, and either attempts to block or stop the attack or reports to a network administrator."
[6] Id. Col. 3, lines 49-50.
[7] Id. Col. 3, lines 51-54
[8] Id. Col. 4, lines 7-9.

processing based on those launched objects described in Yavatkar[9], such a person would neither equate nor confuse remote instantiation of objects with Appellants' claimed querying of data collectors for statistical information.

The examiner has not provided any rational basis upon which one of ordinary skill in the art would construe "statistical information on network packets" with Yavatkar's "gathered information." For example, the examiner states: "**The gathered information is equated to the statistical information because the claim language merely recites statistical information and does not specify the type of statistical information that is collected.**" Appellant limits the type of statistical information to "statistical information on network packets." Yavatkar does not describe statistical information either with the watchdog or the bloodhound agents.

Therefore, Yavatkar does not give the examiner any basis to equate "gathered information" to "statistical information" and in the process clearly misconstrue Yavatkar. Appellant contends that: Yavatkar is clear on what constitutes "the gathered information" – the links or paths traversed by the bloodhound agents.[10]

The examiner also argues that: "**After launching the bloodhound agents the watchdog agents wait for a response (response to what? response to the launching of the bloodhound agents equated to the claimed query). Each bloodhound agents is designed to trace traffics from one type of attack.**"

Appellant contends that the answer to the rhetorical question "**response to what?**" is that the response described in Yavatkar is to the launching of the bloodhound agent; not a response to a query, as claimed. For instance, in steps 422 and 424 of Yavatkar Fig. 9, the bloodhound agent sends a report to the watchdog agent and then the bloodhound agent is destroyed. However, step 422 is not performed in response to a query, but rather is the result of completion of the report.

---

[9] Yavatkar does not describe processing of statistical information. Rather, in one mode Yavatkar mentions that the watchdog agent receives a report (prior to a bloodhound agent self-destructing). The report however is not described as including statistical information on network packets, but instead the links and paths traversed by the bloodhound agents.

[10] Yavatkar Col. 4, lines 10-24. "To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects."

Moreover, the report is not collected "statistical information on network packets." Rather, according to Yavatkar: "The report may indicate the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The report may indicate the failure to find attack traffic on a node.[11]" Therefore, Yavatkar neither describes nor suggests processing statistical information by the watchdog agents or sending statistical information by the bloodhound agents to the watchdog agent in response to queries from the watchdog agent.

The examiner attempts to equate unrelated concepts between Appellant's claims and the teachings in Yavatkar. Appellant contends that it is reversible error *per se* for the examiner to resort to this type of "equivalency"[12] reasoning in the context of an anticipation rejection. "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

Yavatkar fails to disclose the elements of sending queries to data collectors... that ... collect statistical information on network packets sent over the network, the queries to request the statistical information ... and processing the statistical information to determine the source of suspicious network traffic sent to the data center, arranged as in the claim. Therefore, claim 1 is not anticipated by Yavatkar.

Argument B (Claim 2)

Appellant's argument with respect to claim 2 is that Yavatkar neither describes nor suggests "sending queries to the data collectors for the statistical information based on victim destination address." The examiner responds as follows:

> **The bloodhound agents respond to the watchdog agents with the gathered information. The gathered information contains data on the source of the attack and specifically the gateways or nodes (victim) that are allowing the attack traffic. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic. Therefore Yavatkar**

[11] Id. Col. 21, lines 9-14.

[12] The examiner twice resorts to equating features of Appellant's claims to different elements in Yavatkar. "Examiner is equating the launching of the various types of bloodhound agents to launching various types of queries... ." and the examiner also states: "The gathered information is equated to the statistical information .... ."

> **is very much concerned with gathered information based on the gateways destination address (victim destination address) in order to be able to install appropriate firewalls to block the attack traffic and as such meets the scope of the claimed limitation.**[13]

The examiner misconstrues the teachings of Yavatkar. Yavatkar does not describe that the bloodhound agents "respond to" the watchdog agents. Rather, the bloodhound agents are "instantiated by" (i.e., created by) the watchdog agent[14]. The examiner also equates gateways or nodes as "victims." However, the gateways and nodes referred to by the examiner in the portion of reference are not the victims or the target of the attack, but instead are the gateways or nodes that maybe attacking the victim.

The examiner's arguments therefore are not directed to the claimed feature. The claimed feature is: "sending queries to the data collectors for the statistical information based on victim destination address." The claimed feature is not receiving gathered information that contains data on the source of the attack. The examiner argues that: "**Yavatkar is very much concerned with gathered information based on the gateways destination address.**" Appellant contends that concern is not explicitly taught in Yavatkar.

Appellant concedes that network packets include destination addresses and thus Yavatkar inherent possess destination addresses, and indeed, Yavatkar discloses IP addresses of nodes. However, it an unsupportable and impermissible modification of Yavatkar to argue that the reference teaches "sending queries to the data collectors for the statistical information based on victim destination address," as claimed, when Yavatkar fails to mention querying based on IP address or indeed that the bloodhound agents collect send information based on victim destination address.

Yavatkar mentions that: "In step 412, bloodhound agent 116 records the name of the current node (the node's IP address) and the name of the port receiving the most attack traffic (e.g., "Interface 2") in node path list 118."[15] Thus, Yavatkar only teaches to record the IP address of all nodes that the bloodhound agents traverse and place the addresses in a list. In contrast, Appellant's claim 2 is concerned with querying for information based on victim packet

---

[13] Examiner's Answer page 13.
[14] Yavatkar Col. 3, lines 49-52
[15] Id. Col. 20, lines 52-55.

destination addresses not based on IP addresses of nodes that could be involved in an attack on the victim.

Thus while Yavatkar is concerned with the IP address of nodes that the bloodhound agents traverse, Yavatkar does not describe to collect information based on destination address and therefore cannot inherently teach: "sending queries to the data collectors for the statistical information based on victim [data center] destination address."

Argument C (Claim 3)

The examiner argues that:

> **The information gathered on the attack traffic (packets in the network) by the bloodhound agents is equated to the statistical information because the claim language merely recites statistical information on packets in a network and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. The gathered information are processed in order to determine the source of the attack and to diagnose and ultimately try to eliminate the attack. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the claimed limitations.[16]**

Again, the examiner feels justified to equate Appellant's statistical information on packets, with "information gathered on the attack traffic (packets in the network)" because Appellant does not specify: "the type of statistical information that is collected." However, the type of statistical information collected – statistical information on packets in the network – is specified. Appellant need not further specify the type, since Yavatkar clearly does not describe that the bloodhound and watchdog agents operating on any type of statistical information.

Thus, in addition to being reversible error in the context of an anticipation rejection, there is neither an equivalence to nor an inherency of statistical information, as recited in claim 3, with "gathered information," as disclosed by Yavatkar. This conclusion is compelled, because Yavatkar discusses statistical information in the context of distributed collection in the

[16] Examiner's Answer pages 13-14

Background [17] and distinguishes[18] from that approach with the bloodhound and watchdog agents that trace the links and paths traversed by the bloodhound agent.[19] Yavatkar recognizes a distinction between statistical information and the paths and links produced by the bloodhound agents. The examiner errs in ignoring this distinction.

Argument D (Claim 4)

Appellant's Claim 4 deals with processing by the control center. Claim 4 requires: "... a control center that receives the statistical information from the data collectors and includes sending data to/from a gateway device that is associated with the victim data center." The examiner argues that:

> A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. Therefore Yavatkar meets the scope of the clamed limitation.[20]

Appellant replies that to the extent that a watchdog agent can be a "control center", inherently the watchdog agent does not perform the same functions of the claimed control center since the claimed control center operates on "statistical information", whereas Yavatkar only

---

[17] Yavatkar Col. 1, line 65 to col. 2, line 4. "Systems exist for collecting information about network traffic. For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node."

[18] Id. Col. 2, lines 44-50.

[19] Id. Col. 17, lines 17-31

> In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. It may often be the case that a partial path is found ending at the node at which attack traffic enters the network. Such a node may be considered to be the source of the attack traffic--while it is not the originating source, it is the source of the attack traffic to the network. Such information may be used to set up administrative blocks (e.g, a firewall) to prevent attack traffic from entering the network. After collecting this information the bloodhound agent reports to the watchdog agent. In alternate embodiments, the bloodhound agent may collect other information about traffic on the links which it traverses and nodes on which it operates.

[20] Examiner's Answer page 15

discusses that the watchdog agent operates on information pertaining to the paths and links traversed by the bloodhound agents.

Argument E (Claim 6)

Claim 6, limits claim 1, and requires that the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control center in response to the queries sent from the central control center. The examiner argues that:

> **The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator, in an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode. Therefore, Yavatkar's meets the scope of the claimed limitation.[21]**

Claim 6 requires that the queries and the statistical information are sent over a redundant network. Yavatkar does not describe using a network that is different from the network being monitored to report the gathered information and launch the bloodhound agents. The bloodhound agents are instantiated objects. In order for the bloodhound agents to produce a report for the watchdog, the bloodhound agent must operate on the network that the bloodhound is monitoring, because the bloodhound traverses links of that network in order to trace the paths taken by attacking traffic. Therefore, to the extent that the launching of bloodhound agents is equivalent to sending queries, (which Appellant does not concede) Yavatkar cannot describe the claimed features, because in order to gather paths and link information, the bloodhound agents must traverse the network being monitored. In addition, Yavatkar does not describe any other mechanism other than the network being monitored to send reports back to the watchdog agent.

Argument F (Claim 9)

The examiner argues that:

---

[21] Id.

> **The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed limitation.[22]**

Claim 9 includes the feature that if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic from attacking system from reaching the network. Yavatkar is not understood to describe the foregoing feature that the control center issues a request to the gateway.

Argument G (Claim 9)

Appellant's claim 15 adds the feature of receiving from a gateway ... a notification that the victim is under attack, in addition to the features discussed in claim 1.

The Examiner argues that:

> **Yavatkar teaches that the watchdog agent periodically attempts to make a TCP connection to each assigned remote device. If a connection cannot be made, the watchdog agent presumes a TCP attack is occurring with the remote device as a target. Yavatkar further teaches wherein a watchdog agent may also periodically determine reachability to an assigned device, using, for instance, a ping message. That other devices in a network are not reachable may indicate an attack on those devices. The claims merely recite notification and do not specify the type of notification and as such are broadly interpreted. If the watchdog agent can not make TCP connection to a network device or determines that a network device to be unreachable it is presumed to be under attack. The network device notifies the watchdog agent of an attack when it does not establish the TCP connection or it is unreachable. Therefore, Yavatkar meets the cope of the claimed limitation.[23]**

Appellant contends that this argument does not address the features of claim 15. In Appellant's disclosed and claimed system, a gateway may have installed features of detecting DOS attacks. Therefore, according to claim 15, the gateway may detect an attack and inform the control center of the attack. This is not described by Yavatkar. Rather, Yavatkar teaches to

---

[22] Id. page 16
[23] Id. page 17

monitor devices other than what it is operating on. Yavatkar does not make any provision for a watchdog agent receiving from a gateway ... a notification that the victim is under attack.

Argument H (Claim 16)

Claim 16 is directed to the feature of "communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center."

The Examiner contends that:

> **A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. Therefore Yavatkar meets the scope of the clamed limitation.**

Appellant responds that the examiner's arguments do not address the features of claim 16. Claim 16 is directed to communicating statistical information. As discussed above, Yavatkar does mention statistical information as in the Background, but clearly teaches away from that approach in favor of sending a report of paths and links traced by a bloodhound agent. Yavatkar does not mention any feature that would correspond to the watchdog agent sending any information and in particular the claimed statistical information to the bloodhound or to any other watchdog agent. As with many of the arguments raised by the examiner, this argument is directed to features that are not relevant to the claimed subject matter.

Argument I (Claim 17)

Claim 17 further limits claim 15 by reciting: "if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic."

The Examiner argues that:

> **The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the**

> **originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed.[24]**

This argument however again is not directed to the claimed limitation. Yavatkar neither describes nor suggests that the control center issues a request to the gateway to block the attacking traffic.

Argument J (Claim 20)

Claim 20 is directed to a system to thwart denial of service attacks on a victim data center. The system includes a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic and a control center coupled to the plurality of data collectors to receive from the victim site a notification that the victim data center is under an attack and in response ... send queries to data collectors to request the statistical information ... to determine the source of suspicious network traffic ... a gateway device ... disposed to protect the victim data center, and being coupled to the control center. The examiner argues in part:

> **Yavatkar teaches analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process.**
>
> *******
>
> **In step 404 watchdog agent 114 launches bloodhound agent 116 and waits for a response from bloodhound agent 116. (Refer to Yavatkar at col. 19, lines 64-66, emphasis added). The appellant is reminded that the claims must be given their broadest reasonable interpretation. The claim language merely recites sending queries to data collectors...to request statistical information and does not specify the type of query.**
>
> ******** [25]

[24] Examiner's Answer page 19.
[25] Examiner's Answer pages 20-22.

Again, Appellant contends that the examiner's arguments are not directed to the claimed features. The claim requires a system to receive a notification that the data center is under an attack and, in response send queries to data collectors to request statistical information. These features are not described by the arrangement of Yavatkar, in which watchdog agents launch bloodhound agents that send reports on paths/links traversed by the bloodhound agents and thereafter self-destruct or are destroyed.

Argument K (Claim 22)

Claim 22, further limits the system of claim 20, by requiring instructions to determine a source of the attack on the victim data center by analyzing collected statistical information from the data collectors. The examiner argues that:

> **A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem and identify the source of the attack. Therefore Yavatkar meets the scope of the clamed limitation.[26]**

Claim 22 is directed to the feature that the control center determines the source of an attack by analyzing collected statistical information. Again, the examiner's arguments do not address the claimed feature. In the first instance, Yavatkar does not mention that the watchdog determines the source of the attack; that appears to be done, if at all, by the bloodhound agents. Indeed, for reasons discussed above the watchdog is not the analogue to the control center. Moreover, no feature of Yavatkar's described system deals with statistical information. Both Yavatkar and Appellant recognize the difference between statistical information and the path tracing that is described in the Background by Yavatkar. Thus, the examiner improperly conflates and confuses two distinct concepts.

---

[26] Id. page 23.

Argument L (Claim 23)

Claim 23 includes the feature that: "the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack."

The examiner argues:

> **The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed limitation.[27]**

As Appellant argues above, Yavatkar does not disclose any exchange of statistical data between the bloodhound and watchdog agents. Indeed, Yavatkar does not mention that the watchdog agents communicate at all with the bloodhound agents once the bloodhound agents have been launched. While a bloodhound agent sends a report to watchdog agent, this appears to be a onetime event, in that after the report is sent, as least as described in Fig. 9, the bloodhound agent thereafter is destroyed.

Argument M (Claim 24)

Claim 24 includes the feature that data exchanged between the control center and gateway device associated with the victim data center are sent over a redundant network that is a different network than the network that is being monitored by the data collectors. The feature of a redundant network was addressed above in claim 6.

Argument N (Claim 25)

Appellant stands by the argument presented in the brief.

---

[27] Id.

Argument O (Claim 29)

Claim 29 includes the features of instructions to ... receive a notification that the victim data center is under an attack, send queries to data collectors ... the data collectors to sample network traffic and collect statistical information on packets ... the queries to request statistical information from data collectors that have examined network traffic with the victim destination address and determine a source of the attack on the victim data center by analyzing collected information from the data collectors.

The examiner repeats reasoning used in conjunction with claims 1 and 20. However, the examiner does not address the feature of claim 29, not found in claims 1 and 20 that: "queries to request statistical information from data collectors that have examined network traffic with the victim destination address."

The examiner attempts to address "destination address" in answer to Appellant's argument for claim 2.[28] Claim 2 also includes the limitation that the attack involves packets: "that have faked source addresses ... ." The examiner's argument for claim 2 combined with argument for claim 29 fail to show that Yavatkar anticipates this claim.

Yavatkar does not mention "destination addresses" per se. Yavatkar does recognize that packets travel to destinations, but Yavatkar fails to use destination address as a parameter for the queries for statistical information.

Argument P (Claim 30)

For claim 30, both Appellant and the examiner stand by the arguments made for claim 16.

Argument Q (Claim 31)

For claim 31, both Appellant and the examiner stand by the arguments made for claim 9.

[28] The examiner addresses "destination address" in answer to Appellant's argument for claim 2, by arguing that: "Yavatkar is very much concerned with gathered information based on the gateways destination address (victim destination address) in order to be able to install appropriate firewalls to block the attack traffic and as such meets the scope of the claimed limitation."

Argument R (Claim 13 and 14)

Appellant argued:

> Each of claims 13 and 14 are allowable at least because of the features recited in claim 1, since Yavatkar does not anticipate claim 1 and Hill does not cure the deficiencies in Yavatkar as noted in the above argument. Further, the examiner uses Hill to teach "classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2 lines 53-60; col. 6 lines 9-22)." Appellant notes that the teachings in Hill are directed to attack simulation, not to an actual attack or a system to detect and thwart an attack.[29]

The examiner countered:

> **These limitations are not found in the claims. Claimed subject matter not the specification is the measure of the invention. Disclosure contained in the specification cannot be read into the claims for the purpose of avoiding prior art. *In re Sporck*, 55 CCPA 743, 386 F .2d. Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22). The claims merely recite attack and do not specify that the attack be real attacks or attacks that are not simulated. Therefore, Hill's simulated attacks meet the scope of the claimed limitation and render the claims obvious.[30]**

Appellant believes that the examiner may have misunderstood Appellants' arguments. Claims 13 and 14 were argued as allowable over the combination based on the reasoning of claim 1 and that Hill did not cure the deficiencies of Yavatkar.

In addition, Appellant, while believing it unnecessary to address any potential motivation to combine Yavatkar with Hill, pointed out that Hill was directed to attack simulation not to an actual attack .... Appellant's arguments were directed to lack of motivation to combine Hill (attack simulation) with Yavatkar, which was not directed to simulation but rather an actual attack, and thus questioned the existence of any motivation to combine Hill with Yavatkar.

In addition, Appellant's claim 1, the base claim for claims 13 and 14, is directed to "a method of protecting a data center against a denial of service attack," which provides ample

---

[29] Appellant's Appeal Brief page 22.
[30] Examiner's Answer page 28.

support for the argument made of record without incorporation of any limitations from the specification. All of the limitations that Appellant argues are found in the claims.

For these reasons, and the reasons stated in the Appeal Brief, Applicant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 9/5/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21694622.doc